Введение

Из набора всех пар ключей (открытый, секретный) для криптосистемы с открытым ключом RSA некоторые пары ключей обладают свойствами, которые могут быть использованы различными атаками. Некоторые атаки используют слабые места в модуле, а другие используют слабые места в открытом ключе или секретном ключе. Атаки на модуль RSA направлены на обнаружение двух простых множителей (p и q) модуля. Одной из таких атак, является алгоритм атаки Винера.

В 1990 году Майклом Винером был предложен алгоритм атаки на шифр RSA с малым закрытым ключом. А именно шифр RSA обладал уязвимостью: если $p < q < 2p$ и $2d^2 < \frac{m\varphi}{e(p+q)}$ и $e < m$, то d можно было найти как знаменатель подходящей дроби $\frac{e}{m}$, где d – секретный ключ, m – модуль, $\varphi = (p-1)(q-1)$ – функция Эйлера от m, e – открытый ключ, p и q – простые множители m.

Теоритическое обоснование алгоритма атаки Винера и поиск всех параметров шифра RSA

Прежде чем перейти к доказательству состоятельности алгоритма атаки Винера, введем некоторые определения: непрерывное разложение дроби и подходящие дроби.

Пусть m и t два натуральных взаимно простых числа, тогда применив к ним алгоритм Евклида получим непрерывную дробь.

Непрерывная дробь (или цепная дробь) — это конечное или бесконечное математическое выражение вида:

$$\frac{m}{t} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}$$

где a_1 есть целое число, а все остальные a_n— натуральные числа. При этом числа a_1, a_2, a_3, a_4, … называются неполными частными или элементами цепной дроби.

Тогда полученная последовательность [a_1, a_2, a_3, a_4, …] называется непрерывным разложением для дроби $\frac{m}{t}$.

Подходящей дробью для непрерывной дроби называется конечная цепная дробь [a_1, a_2, a_3, … , a_n] значение которой есть некоторое рациональное число $\frac{p_n}{q_n}$

Данные дроби можно вычислить рекуррентным способом:

$p_{-1} = 1,\ p_0 = a_0,\ p_n = a_n p_{n-1} + p_{n-2}$

$q_{-1} = 0,\ q_0 = 1,\ q_n = a_n q_{n-1} + q_{n-2}$

Также для подходящих дробей справедливо свойство:

$\left|\frac{m}{t} - \frac{p}{q}\right| < \frac{1}{2*q^2}$, где $\frac{p}{q}$ подходящая дробь для $\frac{m}{t}$.

Доказательство состоятельности алгоритма атаки Винера:

Верно равенство: $\mathrm{m} - \varphi = \mathrm{p} + \mathrm{q} - 1$

Существует такое целое k что $\mathrm{ed} = 1 + \mathrm{k}\varphi$, тогда верно $\mathrm{k}\varphi < \mathrm{ed}$ следовательно $\mathrm{k} < \frac{\mathrm{ed}}{\varphi}$.

Далее получим:

$\left|\frac{\mathrm{e}}{\mathrm{m}} - \frac{\mathrm{k}}{\mathrm{d}}\right| = \frac{|\mathrm{ed}-\mathrm{km}|}{\mathrm{md}} = \frac{|\mathrm{ed}-\mathrm{k}\varphi+\mathrm{k}\varphi-\mathrm{km}|}{\mathrm{md}}$, так как $\mathrm{ed} - \mathrm{k}\varphi = 1$

далее $\frac{|1+\mathrm{k}(\varphi-\mathrm{m})|}{\mathrm{md}} = \frac{\mathrm{k}(\mathrm{m}-\varphi)-1}{\mathrm{md}} < \frac{\mathrm{k}(\mathrm{m}-\varphi)}{\mathrm{md}} = \frac{\mathrm{k}(\mathrm{p}+\mathrm{q}-1)}{\mathrm{md}} < \frac{\mathrm{k}(\mathrm{p}+\mathrm{q})}{\mathrm{md}}$, а так как $\frac{\mathrm{k}(\mathrm{p}+\mathrm{q})}{\mathrm{md}} < \frac{ed}{\varphi} * \frac{p+q}{md} = \frac{e(p+q)}{\varphi m} < \frac{1}{2d^2}$ исходя из последнего и получаем условие для выполнения алгоритма атаки Винера, а также получаем что d можно найти как знаменатель подходящей дроби $\frac{e}{m}$.

Далее для нахождения параметров p, q применяют такой алгоритм:

Пусть $\mathrm{x} = \frac{\mathrm{p}+\mathrm{q}}{2}$ $\mathrm{y} = \frac{\mathrm{p}-\mathrm{q}}{2}$ тогда $x^2 - y^2 = (x-y)(x+y) = pq = m$

Далее находят такие $\mathrm{x} > \sqrt{\mathrm{m}}$ чтобы $\sqrt{x^2 - m} = y$ было целым числом. Если были найдены параметры p и q, то $\varphi = (p-1)(q-1)$ и m = pq.

Список использованных источников

1. Криптоанализ секретного параметра шифра RSA
   URL: https://goo.su/D8Nfk0Y

2. Факторизация больших целых чисел и криптография
   URL: http://dha.spb.ru/PDF/cryptoFACTOR.pdf

3. Атака Винера на секретный ключ шифра RSA
   URL: https://goo.su/AiKe

3. Атака Винера на шифр RSA
   URL: https://goo.su/ioLxdd